(12) UK Patent Application (19) GB (11) 2 353 885 (13) A

(43) Date of Printing by UK Office 07.03.2001

(21) Application No 0029770.5

(22) Date of Filing 29.04.1999

(30) Priority Data
(31) 09073648 (32) 06.05.1998 (33) US

(86) International Application Data
PCT/US99/09217 En 29.04.1999

(87) International Publication Data
WO99/57625 En 11.11.1999

(71) Applicant(s)
PRC Inc.
(Incorporated in USA - Virginia)
1500 PRC Drive, McLean, Virginia 22102-5050,
United States of America

(72) Inventor(s)
Julie Lynn Huff
Tracy Glenn Shelanskey
Sheila Ann Jackson

(51) INT CL^7
G06F 1/00, H04L 29/06

(52) UK CL (Edition S)
G4A AAP

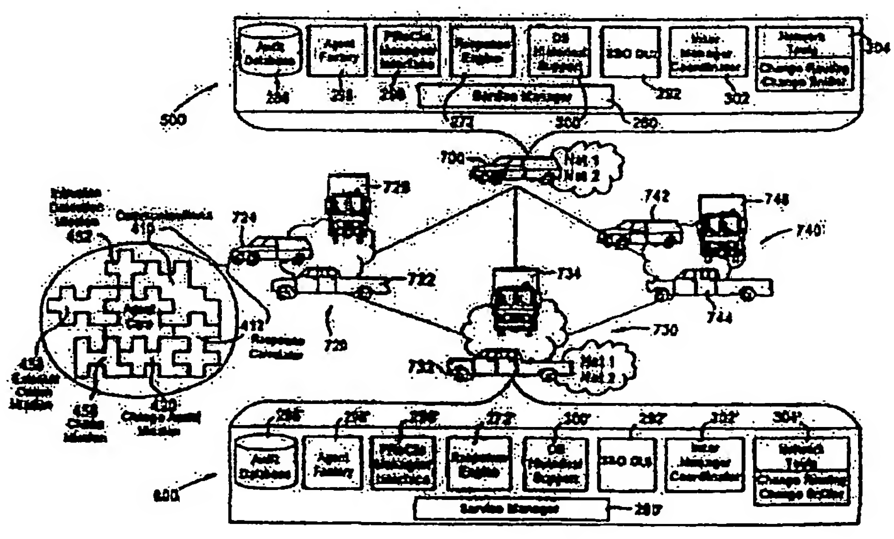
(56) Documents Cited by ISA
WO 94/06096 A
Trans. Inst. of Electron., Information & Comm. Engineers, vol. J81D-I, no. 5, p. 532-539, May 1998
Computers and Security Int. J. devoted to the study of tech. & financ. asp., Vol.17, no.4, 01.01.1998
Computers and Security Int. J. devoted to the study of tech [& financ. asp., Vol.9, no.5, 01.08.1990

(58) Field of Search by ISA
INT CL^6 G06F

(74) Agent and/or Address for Service
Frank B Dehn & Co
179 Queen Victoria Street, LONDON, EC4V 4EL,
United Kingdom

(54) Abstract Title
Dynamic system defence for information warfare

(57) Disclosed is a method and apparatus which includes a security computer system capable of deploying and monitoring software agents on one or more nodes of a network of computers. The agents on each node include a framework agent and either a misdirection mission or a defensive mission. Upon an intrusion detection mission sending information to the security computer system indicative of an actual or suspected misuse or intrusion, the security computer system can automatically take countermeasures against the suspected or actual intrusion or misuse. Automatic countermeasures include using a defensive countermeasure to increase an auditing level conducted by the intrusion detection mission. A misdirection countermeasure mission is used to misdirect requests of the suspected or actual intruder or misuser. An offensive countermeasure is used to send a chase mission to the suspected or actual intruder. The offensive chase mission can either be automatically dispatched with human intervention. The computer sytem includes. a monitor for monitoring by a human system administrator.



GB 2 353 885 A

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00

A1

(11) International Publication Number: WO 99/57625

(43) International Publication Date: 11 November 1999 (11.11.99)

(21) International Application Number: PCT/US99/09217

(22) International Filing Date: 29 April 1999 (29.04.99)

(30) Priority Data:
09/073,648 6 May 1998 (06.05.98) US

(71) Applicant (for all designated States except US): PRC INC. [US/US]; 1500 PRC Drive, McLean, VA 22102-5050 (US).

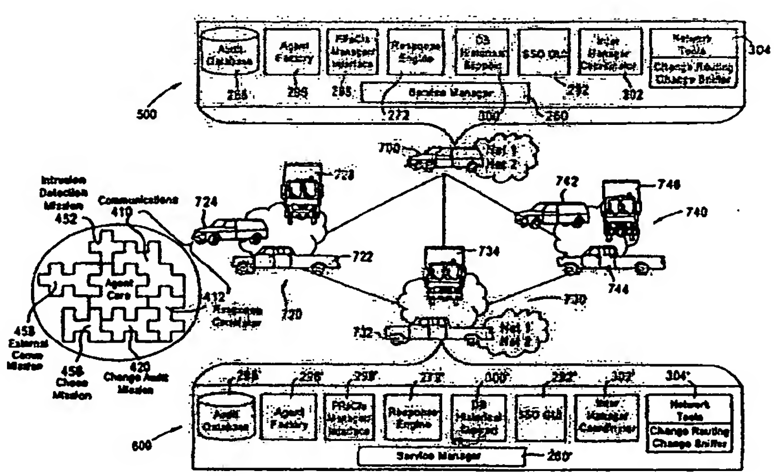
(72) Inventors; and
(75) Inventors/Applicants (for US only): HUFF, Julie, Lynn [US/US]; 4606 Center Street, Omaha, NE 68106 (US). SHELANSKEY, Tracy, Glenn [US/US]; 6211 North 77th Street, Omaha, NE 68134 (US). JACKSON, Sheila, Ann [US/US]; 7212 South 38th Street, Omaha, NE 68147 (US).

(74) Agent: BERNER, Kenneth, M.; Lowe Hauptman Gopstein Gilman & Berner, LLP, Suite 310, 1700 Diagonal Road, Alexandria, VA 22314 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: DYNAMIC SYSTEM DEFENCE FOR INFORMATION WARFARE



(57) Abstract

Disclosed is a method and apparatus which includes a security computer system capable of deploying and monitoring software agents on one or more nodes of a network of computers. The agents on each node include a framework agent and either a misdirection mission or a defensive mission. Upon an intrusion detection mission sending information to the security computer system indicative of an actual or suspected misuse or intrusion, the security computer system can automatically take countermeasures against the suspected or actual intrusion or misuse. Automatic countermeasures include using a defensive countermeasure to increase an auditing level conducted by the intrusion detection mission. A misdirection countermeasure mission is used to misdirect requests of the suspected or actual intruder or misuser. An offensive countermeasure is used to send a chase mission to the suspected or actual intruder. The offensive chase mission can either be automatically dispatched with human intervention. The computer sytem includes a monitor for monitoring by a human system administrator.

DYNAMIC SYSTEM DEFENSE FOR INFORMATION WARFARE

Field of the Invention

The present invention relates generally to intrusion detection systems for computer systems, and more particularly, relates to intrusion detection systems having dynamic response capabilities for suppressing and automatically taking countermeasures against suspected and actual intruders and misusers.

Background of the Invention

The development of the computer and its astonishingly rapid improvement have ushered in the Information Age that affects almost all aspects of commerce and society. Just like the physical infrastructures that support the American economy, there is a highly developed computer infrastructure that supports the American and worldwide economy.

Besides traditional physical threats to United States security, the security of the United States is also dependent on protecting the computer infrastructure that supports American government and industry. The computer infrastructure is open to attack by hackers and others, who could potentially wreak havoc.

The President of the United States has recognized the existence of these infrastructures and has created the President's Commission on Critical Infrastructure Protection. This Commission was constituted to determine which industries are critical and whether these industries were vulnerable to cyber attack. The Commission issued a report and deemed transportation, oil and gas production and storage, water supply, emergency services, government services, banking and finance, electrical power and telecommunications to be critical infrastructures which rely on the computer infrastructure.

Another type of unauthorized operation is called a misuse. A misuse is an unauthorized access by a computer within the secure network. In a misuse situation, there is no breach of the firewall. Instead, a misuse occurs from inside the secure computer network. A misuse can be detected when an authorized user performs an unauthorized, or perhaps, infrequent operation which may raise the suspicion that the authorized user's computer is being misused. For example, an unauthorized user could obtain the password of an authorized user and logon to the secured network from the authorized computer user's computer and perform operations not typically performed by the authorized user. Another example might be where a terrorist puts a gun to the head of an authorized user and directs the authorized user to perform unauthorized or unusual operations.

There are systems available for determining a breach of computer security which can broadly be termed intrusion detection systems. Existing intrusion detection systems can detect intrusions and misuses. The existing security systems determine when computer misuse or intrusion occurs. Computer misuse detection is the process of detecting and reporting uses of processing systems and networks that would be deemed inappropriate or unauthorized if known to responsible parties. An intrusion is an entry to a processing system or network by an unauthorized outsider.

These existing computer security systems have audit capabilities which are passive. These systems collect audit information from network devices and format those audits for review. Most of the existing computer security systems known to the inventors do not take steps to stop the misuse or intrusion after it is detected. Those that do take active steps are limited to logging a user off the network, stopping communications with that computer halting operations or other forms of notification such as a message to the security officer. Manual countermeasures are necessary. Once a hacker or intruder enters a critical system computer, even if detected, the hacker may do considerable harm before an operator of the system can react and initiate an appropriate, manual countermeasure, to stop the misuse or intrusion or to positively identify the

software module which is capable of being transported from one computer to another under instruction from the security computer. The security computer receives information from agents who perform the functions of monitoring the computers on the network for misuse and intrusion and send information to the security computer indicative of suspected or actual intrusions or misuses. The security computer can then take defensive and/or offensive measures to suppress or counterattack the intruder or misuser by automatically sending defensive or offensive agents to the computer on which a suspected or actual intrusion or misuse occurred. The security computer includes a monitor for monitoring by a human system administrator.

These and other objects of the present invention are achieved by a method for a computer network including receiving information, at a security computer, that an unauthorized operation has occurred at a computer on the network. Based on this information, countermeasures are initiated automatically, from the security computer, against the unauthorized operation where the determined unauthorized operation occurred.

These and other objects of the present invention are achieved by a method for a computer network including receiving information, at a security computer, that an unauthorized operation has occurred at a computer on the network. Based on this information, countermeasures are taken from the security computer against the intrusion. The countermeasures include dispatching a transferable self-contained set of executable instructions to the identified audited computer and executing the set of executable instructions on the identified audited computer to implement the countermeasure.

These and other objects of the present invention are achieved by a computer network comprising a security computer including one or more software modules for deploying, controlling and monitoring agents on one or more nodes of the computer network. Each of the one or more computers on the computer network includes a security operative which includes at least one offensive

stored thereon at least one offensive agent for taking countermeasures against an actual or suspected intruder to prevent or suppress further intrusion by the actual or suspected intruder.

Still other objects and advantage of the present invention will become readily apparent to those skilled in the art from following detailed description, wherein the preferred embodiments of the invention are shown and described, simply by way of illustration of the best mode contemplated of carrying out the invention. As will be realized, the invention is capable of other and different embodiments, and its several details are capable of modifications in various obvious respects, all without departing from the invention. Accordingly, the drawings are to be regarded as illustrative in nature, and not as restrictive.

Brief Description of the Drawings

The present invention is illustrated by way of example, and not by limitation, in the figures of the accompanying drawings, wherein elements having the same reference numeral designations represent like elements throughout and wherein:

Figure 1 is a high-level block diagram of an exemplary secured computer network on which the present invention can be implemented;

Figure 2 is a high-level block diagram of an exemplary computer system with which the present invention can be implemented;

Figure 3 is a block diagram of a logical architecture of the system according to the present invention;

Figure 4 is an illustration of a display screen depicting the status agents on nodes on a computer network; and

Figure 5 is a diagram of a first embodiment of the invention as used on several fleets of trucks in a wireless network.

A security server 114 for implementing the intrusion detection, suppression, and countermeasure system according to the present invention is coupled to the network cable 102. A firewall 116 connects the secure network 100 to an interface 118. The firewall 116 is a combination hardware and software buffer that is between the internal network 100 and external devices outside the internal computer network 100. The network devices within the internal network 100 appear within the dashed lines in Figure 1, and the external devices outside the internal network appear outside the dashed lines in Figure 1. The firewall 116 allows only specific kinds of messages from external devices to flow in and out of the internal network 100. As is known, firewalls are used to protect the internal network 100 from intruders or hackers who might try to break into the internal network 100. The firewall 116 is coupled to an interface 118. The interface 118 is external to the network 100 and can be a modem or an Internet Protocol (IP) router and serves to connect the secure network 100 to devices outside the secure network. For illustrative purposes, an intruder computer system is depicted at 130.

Figure 2 is a block diagram illustrating an exemplary computer system, such as the personal computer 112 depicted in Figure 1, usable on the internal secure network 100. The present invention is usable with currently available personal computers, mini-mainframes, mainframes and the like. Although computer 112 is depicted in Figure 1 as a network device which is part of a wired local network, the computer 112 is also envisioned as being connected to the network 100 by a wireless link. In this regard, the computer 112 is usable in the cockpit of an aircraft, on a ship and in moving land vehicles. It is believed that the invention described herein can readily be adapted for specific hardware configurations for each of these operating environments.

Computer system 112 includes a bus 202 or other communication mechanism for communicating information, and a processor 204 coupled with the bus 202 for processing information. Computer system 112 also includes a main memory 206, such as a random access memory (RAM) or other dynamic storage

described below. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.

Computer system 112 also includes a communication interface 218 coupled to the bus 202. Communication interface 218 provides a two-way data communication as is known. For example, communication interface 218 may be an integrated services digital network (ISDN) card or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface 218 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. In the preferred embodiment the communication interface 218 is coupled to the network cable 102. Wireless links may also be implemented. In any such implementation, communication interface 218 sends and receives electrical, electromagnetic or optical signals which carry digital data streams representing various types of information. Of particular note, the communications through communication interface 218 may permit transmission or receipt of the intrusion detection, suppression and countermeasure agents for taking countermeasures against suspected or actual intruders or misusers.

The logical architecture of one embodiment of the suppression and countermeasure system 250 of the present invention is illustrated in Figure 3 and can be implemented on the physical network described above and depicted in Figure 1. The suppression and countermeasure system 250 of the present invention includes two building blocks: a service manager 260 on the network security server 114 and dispersed security operatives 320, 322, 324. As discussed in detail below, the network security server 114 is located on one or more computers in the secure network 100 and the security operatives 320, 322, 324 are located at remote computers within the network 100 and dispatched, controlled and monitored by the security server 114.

mode can capture information including a packet header having the address of another computer. The inter manager coordinator 304 manages communications to other additional service managers 260. In a wireless network without the firewall 116, the network cable 102 could be a wireless path or a combination of wired and wireless paths. For example, in a non secured environment, the signal path 102 could be the Internet.

The service request processor module 290 dispatches the dispersed security operatives 320, 322, 324 to other network devices such as servers 104, 106, host 108, terminal 110, and PC 112. The service request processor module 290 also initiates the instantiation of the security operatives 320, 322, 324 on the remote computers. Each network device has a security operative residing thereon. For simplicity, in Figure 3, only the security operatives 320, 322, 324 are depicted which reside at the host 108 and PC 112, respectively.

An intruder system is depicted as the block 130 in Figure 1. The intruder, by definition, must be outside the secured network. Of course, the intruder 130 does not form a part of the present invention but is being shown for illustrative purposes only. The intruder is often a hacker. An intruder 130 can use a PC with a modem or other communication link. For purposes of this patent application, it can be assumed that even though the firewall 116 provides some degree of protection, hackers will be able to gain access to one or more of the devices on the network 100 and thus intrude into the secured network 100. By contrast, a misuser is using a network device from within the secured network 100.

Each network device such as server 104, host 108 and PC 112 usually will be referred to herein as nodes. As used herein, a node is an addressable point on a network. A node can connect a computing system, a terminal, or various other peripheral devices to the network. Nodes 104, 108, 112, for example, can communicate with each other via signal path 102.

Alternatively, instead of networking computers 104, 108, 112 via signal path 102, there can be individual signal paths between each computer and the security server 114. Additionally, the security server 114 can also be in

processing module 288 and the nodes 104, 108, 112 occurs through a respective communication framework 410.

As depicted in Figure 3, the security operatives 320, 322, 324 each include missions such as an audit and intrusion detection mission 452, a change audit mission 454, and a chase mission 456, which are discussed in detail below. Like the communication framework 410, these missions preferably are Java agents. To configure a mission at a communication framework 410, the service request processor module 290 sends a reconfiguration segment to a particular node on the network where the mission is to be deployed. The reconfiguration segment is then instantiated as the mission under instructions from the service request processor module 290.

As will be explained below, many other missions are possible. The agents can be also written in many languages such as C++, C and assembler and other languages known to those of skill in this art.

It should be noted that different or common entities may control the secure network 100 and nodes 104, 108 and 112. For example, network 100 and nodes 108, 112 may be owned by one company or the military and thus are under the control of one entity. Alternatively, different entities may control the network 100 and each of the nodes. For example, a system administrator may control the network 100 and each of the nodes 104, 108, 112 is owned by different companies who might be concerned about preventing a cyber attack and responding to a cyber attack.

It is important that the communication framework 410 and agent core framework 420 have full permission to use and access every resource on the host computer 108 or 112, to append, delete, modify, and rewrite files. In a UNIX environment, for example, the communication frameworks 410 and agent core framework 420 would reside at the root access level and thus have full permission to use every resource on the host UNIX computer. The communication framework 410 tracks missions and sends and receives them from one port to another. The communication framework 410 also enables missions to

Thus, the service request processor module 290 remotely controls the frameworks 410 and 420 and each of the missions 452, 454, 456, 458. Besides starting a mission by having the mission instantiated at a node, the service request processor module 290 also tracks each instance of each mission. This is achieved by having the agent core framework 420 periodically send information to the service request processor module 290 regarding the currently active missions acting at that node.

Once the frameworks 410 and 420 are in place at each of the nodes, the service request module 290 can deploy data collection agents such as intrusion detection mission 452, and collect data from data collection agents and store the collected data in the audit database storage unit 286. The service request processor module 290 can send a new mission to a communication framework 410 on a node as instructed by the network tools module 302.

User profile data is stored in the audit database storage unit 286. This data may be used to detect an intrusion. For example, a user may have access to a particular database but has not accessed the database for over a year. The sudden access of the database may be inconsistent with the user profile as determined by the network tools module 302. This may be an alert that a misuse might be occurring but because the user is performing a legal operation the network tools module 302 may direct the service request processor module 290 to increase the auditing level being performed by the intrusion detection mission 452 and send out a change audit mission 454.

The service request processor 290 provides for system protection which might include shutting down a node when a suspected intrusion occurs or when a node has been subverted. Another type of system protection may be when an agent or mission does not report back for a certain period of time and it may be assumed that the agent or mission has been killed or subverted. Subverted means that the system, agent or mission has been killed or corrupted by an intruder or misuser.

provide information regarding suspected or actual intrusions or misuses. The software agents implementing these missions perform defensive activities to determine the possible existence of a security breach. These missions are informational missions. Information obtained from these missions can be used to obtain a warrant. The second mission category is the "misdirection" category which includes the misdirection mission 458. The software agent of a misdirection mission redirects requests for data from a suspected or actual intruder or misuser, typically to a dummy database that has been set up to keep the suspected intruder or misuser from accessing useful information. The third mission category is the "offensive" category, where an agent is dispatched to a computer on which a suspected or actual intruder resides. Once the agent is deployed at the intruder's computer, an offensive agent can be used to obtain information about the suspected intruder or be used to disable the intruder.

All missions report back to the message processing module 288 periodically. When the response engine module 272 detects a suspected intrusion or misuse or an actual intrusion or misuse, then the response engine module 272 alerts the service request processor module 290, which request the agent factory module 296 dispatch an additional mission.

As previously mentioned, the communications framework 410 and the agent core framework 420 at each node has the intrusion detection mission 452, the change audit mission 454, and the chase mission 456, and on the node 112 the frameworks 410 and 420 also have the misdirection mission 458. It should be understood that the present invention is not limited to the exemplary missions described herein but many other missions and combinations of missions within each node are possible.

The audit intrusion detection mission 452 can be a specially developed software program as described in a copending U.S. patent application entitled "Method and System for Normalizing Audit Trail Records Received from Heterogeneous Sources" and "Method and System for Detecting Intrusion into and Misuse of a Data Processing System" both of which are assigned to the

intrusion or misuse. Any type of anomalous behavior may warrant additional auditing of a computer node before taking any other defensive or offensive countermeasures. As mentioned previously, because of the speed of a cyber attack, more frequent auditing may be required to detect a cyber attack once a suspected or actual intrusion or misuse is detected.

The chase mission 456 is an offensive agent which is deployed by the response engine module 272 or by the audit and intrusion detection module 452 instructing the service request processor 290 to dispatch the chase mission 456 to the node from which the suspected intrusion is taking place. As depicted in Figure 3 the intruder is 130. The chase mission 456 can send back to the service manager 260 information regarding the suspected intruder including the suspected intruder's address and information contained on the suspected intruder's computer, and other information.

The misdirection mission 458 might include a "Trojan horse" which could be downloaded to place a chase mission 456 in the suspected intruder 130. The Trojan horse is a subversive device placed within the computer system of the suspected intruder. A Trojan horse is advantageous because it is possible for a hacker to disguise the address where the hacker is located. Thus, it may not be possible to directly send the chase mission 456 to the hacker. Instead, it may be necessary to use a Trojan horse which is unknowingly downloaded by the hacker and thus the chase mission 456 can be sent to the computer which the hacker is using. The chase mission 456 will frequently reside within a dummy database 460 created by the misdirection mission 458 and will be downloaded by the suspected intruder 130 and the chase mission 456 will thus travel to the computer system of the suspected intruder. The chase mission 456 can then send information regarding the location of the suspected intruder and information about the suspected intruder to the message processing module 288. The chase mission 456 being within the Trojan horse is very useful because it is often difficult to determine the address of the suspected or actual intruder. Thus, it may be necessary to have the suspected or actual intruder download the Trojan horse

modules 286, 296, 298, 272, 300, 292, 302, 304 and computer system 600 includes modules the same modules referenced with an asterisk. Each vehicle serves as a node on the two wireless system networks NET1 and NET2. As depicted in Figure 5, there is one system network NET1 on which communication is conducted on a first frequency. There is a second network NET2 on which communication is conducted at a second frequency. There are three peer-to-peer links 720, 730, 740 within NET1 and NET2 and the truck 700. The truck 700 can communicate over wireless links to the three other three peer-to-peer links 720, 730, 740 in a known manner.

The peer-to-peer link 720 includes a truck 722, a van 724 and a truck 726, each of which is in wireless communication with each other. One of the vehicles 722, 724, 726, can serve as a central hub for communication with the other peer-to-peer links 730, 740 and the truck 700. Communication from vehicles not serving as the hub to other networks would go through the vehicle serving as the hub. Peer-to-peer communication can occur between vehicles 722, 724, 726.

The second peer-to-peer link 730 includes a truck 732 and a van 734. As in the first network, peer-to-peer wireless communication can occur between each of these vehicles. One of these vehicles would serve as the hub for communication with other peer-to-peer links 720, 740 and the truck 700.

The third peer-to-peer link 740 includes a van 742, a truck 744 and a truck 746. As before, peer to peer wireless communication can occur between each of these vehicles and communication with other networks occurs with the vehicle designated as the central hub. Truck 732 carries the computer system 600.

The computer systems 500, 600 on the trucks 700 and 732 can monitor each of the other vehicles in the network for intrusion or misuse as described above with respect to the security server 114 in Figure 3. Each vehicle 722, 724, 726, 728, 734, 736, 742, 744, 746 would contain a computer system, such as that described above as host 112, and supporting wireless communication devices. Each computer system on a vehicle would have frameworks 410 and 420 and at least one mission. As depicted in Figure 5, the van 724 includes missions 452-

What is Claimed Is:

1. A method for computer network use, comprising:

receiving information, at a security computer, that an unauthorized operation has occurred at a computer on the network; and

initiating an automatic countermeasure, from the security computer, against the unauthorized operation at the audited computer where the determined unauthorized operation occurred.

2. The method of claim 1, comprising:

auditing operations on computers on the computer network for unauthorized operation and providing information from the one or more audits to a security computer on the network; and

determining, based upon the information provided by the auditing step, that an unauthorized operation has occurred at an audited computer.

3. The method of claim 1, wherein said initiating a countermeasure step includes the step of sending a transferable self-contained set of executable code instructions for implementing the countermeasure from the security computer to the computer on which the determined unauthorized operation occurred.

4. The method of claim 3, wherein said transferable self-contained set of executable code is an agent.

5. The method of claim 2, wherein said auditing step is performed by an audit and intrusion detection mission on a computer on the network which provides audit information to the security computer that an unauthorized operation has occurred.

6. The method of claim 1, wherein said initiating a countermeasure step includes deploying a transferable self-contained set of executable code instructions at the computer on which a determined unauthorized operation

15. The method of claim 1, comprising instantiating defensive and offensive agents at each of the one or more computers.

16. A method for computer network use, comprising:

receiving information, at a security computer, that an unauthorized operation has occurred at a computer or the network; and

taking a countermeasure, from the security computer, against the intrusion including dispatching a transferable self-contained set of executable instructions to the identified audited computer, and automatically executing the set of executable instructions on the identified audited computer to implement the countermeasure.

17. The method of claim 15, auditing computers on the computer network and providing information from the one or more audits to a security computer on the network, and determining, based upon information provided by the auditing step, that an unauthorized intrusion has occurred at an identified audited computer.

18. The method of claim 15, wherein the taking a countermeasures step occurs automatically.

19. A computer network comprising:

a security computer including one or more software modules for deploying, controlling and monitoring agents on one or more computers of the computer network;

each of said one or more computers on the computer network including a security operative which includes:

a memory coupled to said processor storing executable code for taking countermeasures, the memory having stored therein sequences of instructions, which, when executed by said processor, cause said processor to perform the steps of:

receiving information that an unauthorized operation has occurred on a computer on the network;

taking countermeasures against the unauthorized operation including dispatching a transferable self-contained set of executable instructions to the determined computer; and executing the set of executable instructions on the determined audited computer to implement the countermeasure.

26. A security computer architecture comprising:

receiving means for receiving information that an unauthorized operation occurred on the computer network;

determining means for determining that an unauthorized operation has; and

countermeasure means for automatically initiating countermeasures against an unauthorized operation at the audited computer.

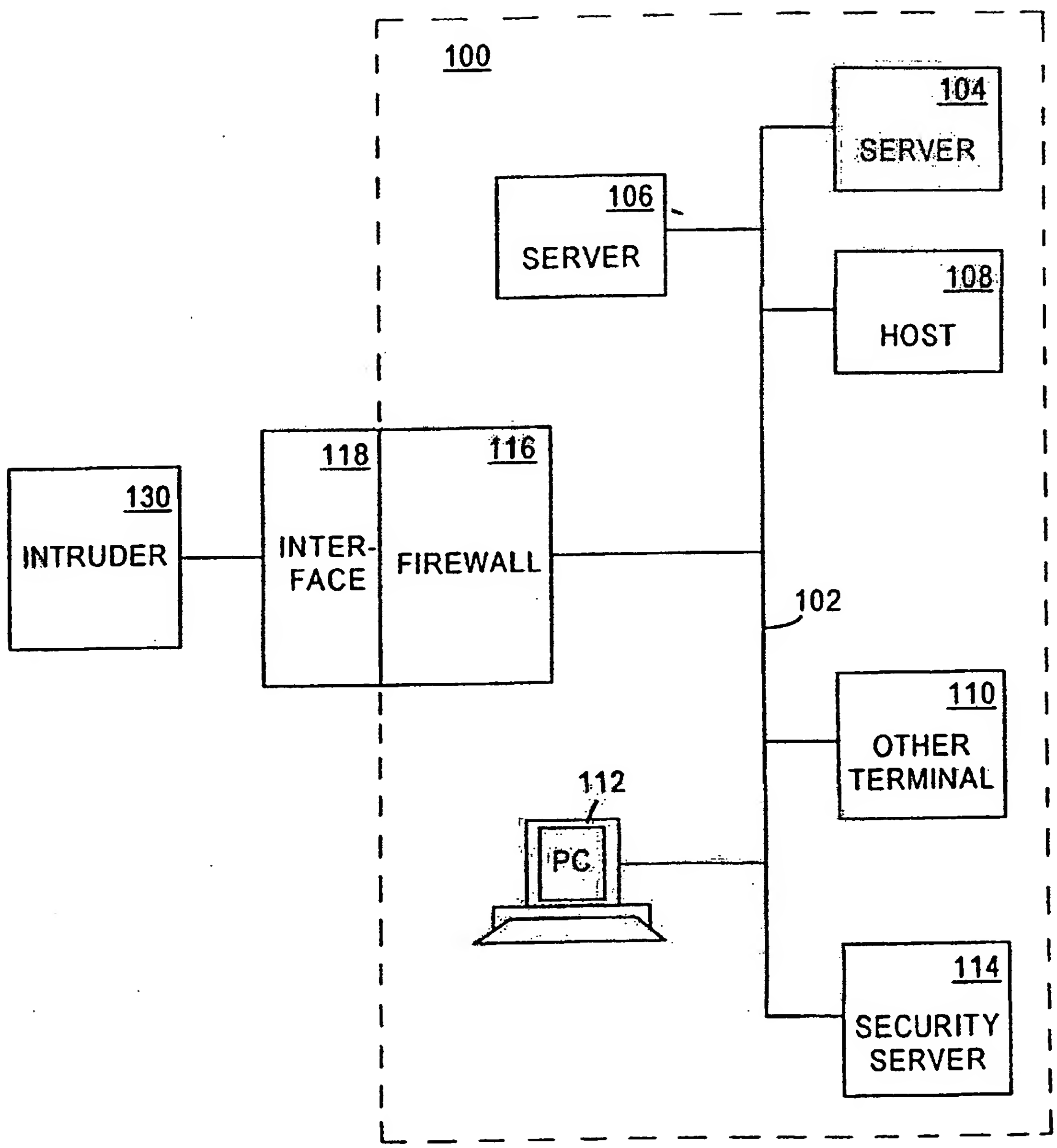
27. A computer readable medium having agents stored thereon, the agents comprising:

at least one defensive agent for monitoring for unauthorized operations on a computer within a computer network and reporting back to a security computer;

at least one misdirection agent for misdirecting requests by an actual or suspected intruder or misuser to a location in a monitored computer where the actual or suspected intruder obtains false information; and

at least one offensive agent for taking countermeasures against an actual or suspected intruder to prevent or suppress further intrusion by the actual or suspected intruder.

FIG. 1


100
104
SERVER
106
SERVER
108
HOST
118
116
130
INTRUDER
INTER-
FACE
FIREWALL
102
110
OTHER
TERMINAL
112
PC
114
SECURITY
SERVER

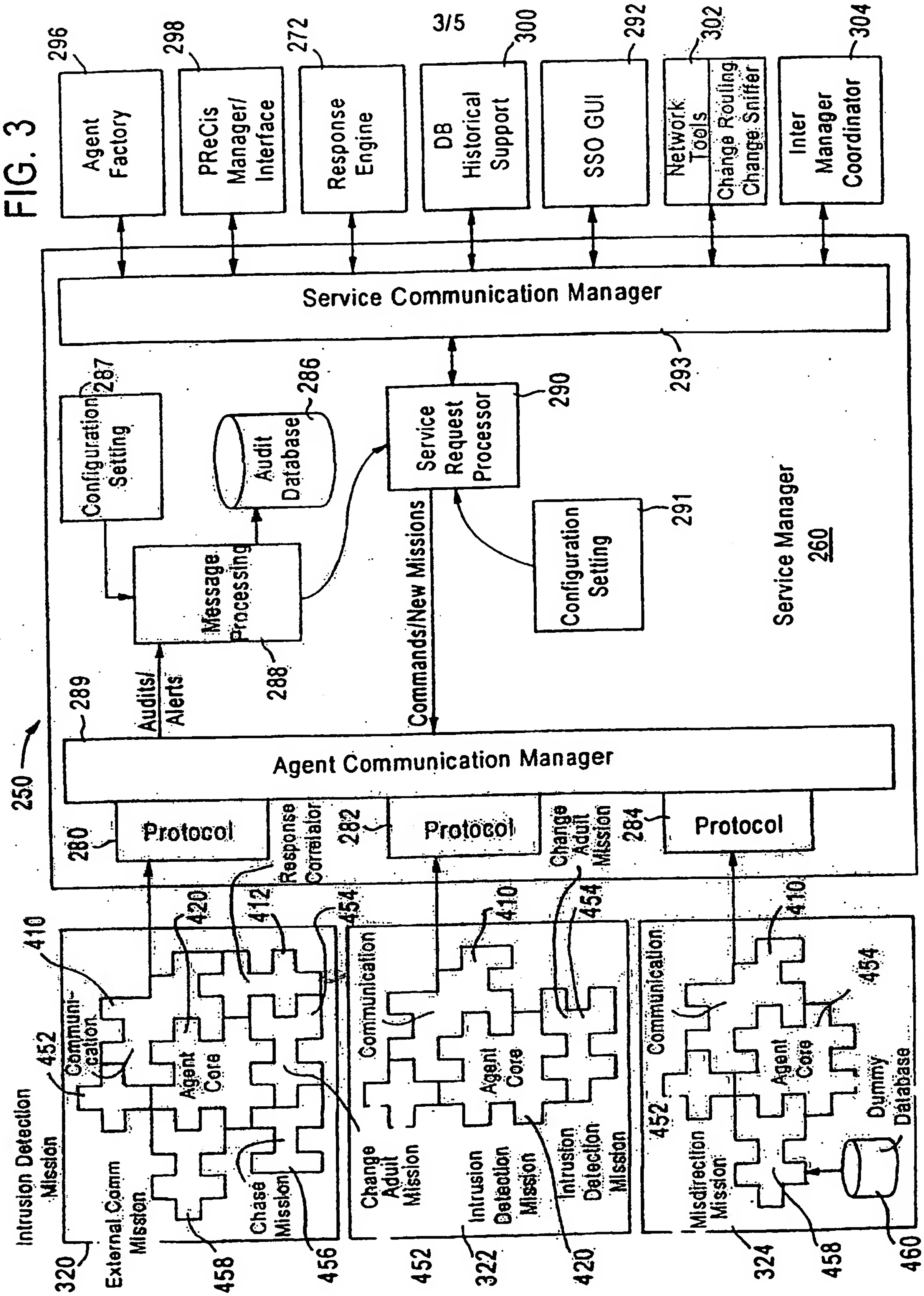

Agent Factory
296
PReCis Manager/ Interface
298
Response Engine
272
DB Historical Support
300
SSO GUI
292
Network Tools
Change Routing Change Sniffer
302
Inter Manager Coordinator
304
Service Communication Manager
293
Configuration Setting
287
Audit Database
286
Service Request Processor
290
Configuration Setting
291
Message Processing
288
Audits/ Alerts
Commands/New Missions
Service Manager
260
250
289
Agent Communication Manager
280
Protocol
Response Correlator
282
Protocol
Change Adult Mission
284
Protocol
Intrusion Detection Mission
320
External Comm Mission
452
Communi- cation
410
Agent Core
420
412
454
Chase Mission
458
456
Communication
410
454
Agent Core
Change Adult Mission
452
Intrusion Detection Mission
322
Intrusion Detection Mission
420
Communication
410
454
Agent Core
452
Dummy Database
Misdirection Mission
324
458
460

FIG. 3

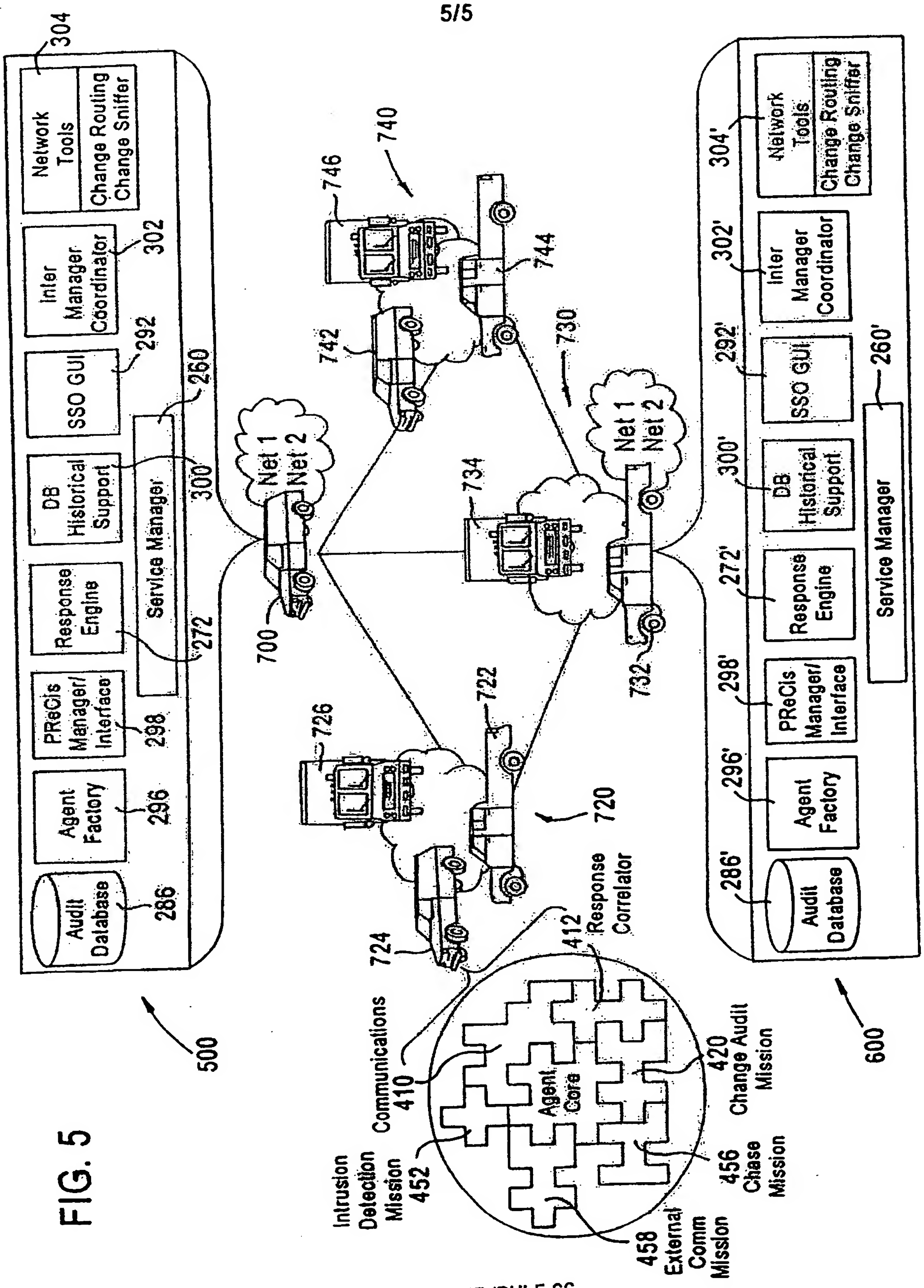

304
Network Tools
Change Routing
Change Sniffer
Inter Manager Coordinator
302
SSO GUI
292
260
DB Historical Support
300
Service Manager
Response Engine
272
PReCis Manager/ Interface
298
Agent Factory
296
Audit Database
286
500
740
746
744
742
730
Net 1
Net 2
734
700
732
726
722
720
724
412
Response Correlator
Communications
410
Agent Core
420
Change Audit Mission
Intrusion Detection Mission
452
456
Chase Mission
458
External Comm Mission
304'
302'
292'
260'
300'
272'
298'
296'
286'
600

FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/09217

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	LABUSCHAGNE L ET AL: "The Use of Real-Time Risk Analysis to Enable Dynamic Activation of Countermeasures" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 17, no. 4, 1 January 1998 (1998-01-01), page 347-357 XP004129259 ISSN: 0167-4048 page 353, paragraph 3.4 - page 356, left-hand column, paragraph 1; figures 7-9	1,2,11, 15-19, 25-28
A	MCKOSKY R A ET AL: "A File Integrity Checking System to Detect and Recover from Program Modification Attacks in Multi-User Computer Systems" COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 9, no. 5, 1 August 1990 (1990-08-01), pages 431-446, XP000147838 ISSN: 0167-4048 page 438, paragraph 3.4 page 445, paragraph 5.3; figures 7-9	1,2,5, 10,11, 16-19, 25-28
A	WO 94 06096 A (TRUSTED INFORMATION SYSTEMS INC.) 17 March 1994 (1994-03-17) page 27, line 6 - page 29, line 25; figures 6-8	1,2,10, 16,17, 19,25,26

1